Antwoord VTC op een vraag van een lokale overheid n.a.v. een debat over CLOUD.

Dit antwoord wordt bijgetreden door de POD Maatschappelijke Integratie.

In het groen wat gesteld werd door de VTC op het debat (Shopt-IT van V-ICT-OR 2014). Er werd meer uitleg bijgezet wegens de vraag later gesteld werd:
(De vraag was: *"Als ik het goed begrepen heb zijn wij als overheid momenteel niet gerechtigd applicaties te draaien bij Amerikaanse cloudproviders (indien deze persoonsgegevens bevatten). Is dit een richtlijn/advies of effectief een Europese/Belgische wet? Dit lijkt mij een zeer belangrijk onderscheid, aangezien binnen onze organisatie toch steeds meer de tendens ontwikkelt om externe hosting en/of cloudoplossingen te overwegen."*
De reactie van de vraagsteller op het antwoord ivm overheidscloud was de volgende: "*Dit lijkt me inderdaad de beste (misschien niet voor de hand liggende) oplossing : Eigen Europese/Belgische datacenters, wellicht draaiend op niet Europese hardware en besturingssystemen, maar wel in eigendom van …*")

Het antwoord van de VTC:
Wat de huidige toepasselijke wettelijke bepalingen betreft, kan inzake persoonsgegevens gewezen worden op artikel 16, §4 van de wet verwerking persoonsgegevens (ook 'privacywet' genoemd) waarin staat dat de verantwoordelijke voor de verwerking, alsmede de verwerker, de gepaste technische en organisatorische maatregelen treffen die nodig zijn voor de bescherming van de persoonsgegevens[1] Zie hiervoor ook het artikel 17 van de Europese privacyrichtlijn[2].

Er worden door de cloudaanbieders inspanningen [3]geleverd inzake beveiligde verbindingen en encryptie van de data wordt aangeboden (mogelijk wel niet standaard of zonder extra kost) voor vertrouwelijke gegevens. Het is echter niet zeker of de geboden oplossingen de gepaste bescherming bieden.[4] Wie heeft de sleutel? garanties om na lange termijn terug te kunnen de-encrypteren? eenvoudig en snel in gebruik (want anders wordt het toch niet toegepast)? …

---

[1] "§ 4. Om de veiligheid van de persoonsgegevens te waarborgen, moeten de verantwoordelijke voor de verwerking, en in voorkomend geval zijn vertegenwoordiger in België, alsmede de verwerker, de gepaste technische en organisatorische maatregelen treffen die nodig zijn voor de bescherming van de persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens.
Deze maatregelen moeten een passend beveiligingsniveau verzekeren, rekening houdend, enerzijds, met de stand van de techniek ter zake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen gegevens en de potentiële risico's."

[2] "2. De Lid-Staten bepalen dat de voor de verwerking verantwoordelijke, in geval van verwerking te zijnen behoeve, een verwerker moet kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerking en moet toezien op de naleving van die maatregelen."

[3] http://www.nutech.nl/internet/3720907/google-vrij-zeker-data-onbereikbaar-overheden.html
(opm: lijkt op basis van wetgeving van toepassing op Amerikaanse burgers).
Microsoft zou ook encryptie aanbieden. Dat werd door hen gezegd op shopt-it na de opmerkingen van de veiligheidsexperts in het debat.

[4] Zie oa (uit 2011) http://www.computable.nl/artikel/achtergrond/security/4046361/1276896/deel-1-encryptie-gevoelige-clouddata-is-noodzakelijk.html

Het is positief dat de cloudleveranciers informatieveiligheid als een verkoopsargument beginnen te gebruiken.
Op dit moment is het zo dat enkele grote cloudaanbieders op dat punt haasje over spelen en is het niet duidelijk welke de beste of voldoende garanties biedt.

Commerciële bedrijven zouden er ook aan denken om diensten of producten aan te bieden voor het opzetten van een private (of hybride?) cloud, waarbij de infrastructuur en dus ook de data in handen van de eigen organisatie blijven.[5]

Bij de commerciële cloudaanbieders beweegt er dus wat, maar ook aan de zijde van de overheid. Enkele overheden in België hebben zelf al een private (of community?) cloud opgezet[6]. Er zouden ook plannen zijn voor intergouvernementele samenwerking binnen Europa.

Daarbij aansluitend kan verwezen worden naar de "Good Practice guide for securely deploying Governmental Clouds"[7] van het European Union Agency for Network and Information Security (ENISA) waarin talrijke aanbevelingen staan inzake privacybescherming en informatieveiligheid.

Conclusie: aangezien er wat groeit qua beveiliging en vertrouwelijkheid, maar er tegelijk nog veel onzekerheden zijn, is het aangewezen geen overhaaste beslissingen te nemen.

Ter herinnering de belangrijkste problemen inzake publieke cloud op een rijtje:

- gebruik van de data voor het opstellen van profielen van de gebruikers die dan voor eigen marketingdoeleinden gebruikt worden (cf. recent ivm een Nederlandse en een "Belgische" bank[8]), doorgegeven worden aan "verbonden ondernemingen" of verkocht worden;[9]

- hacking en achterdeurtjes[10] en hiermee gelinkt:

- NSA spionageactiviteiten (NSA al dan niet op basis van de hieronder vermelde Amerikaanse wetgeving) via de firma's die de clouddiensten aanbieden (en daar nu niet gelukkig lijken mee te zijn[11]).

- aandachtspunten bij cloudcontracten en outsourcingcontracten in het algemeen, Zie ondermeer publicatie van ENISA[12] en de al talrijke richtlijnen gepubliceerd door advocaten en consultants.

---

[5] http://datanews.knack.be/ict/nieuws/hp-pompt-miljard-dollar-in-open-cloud/article-4000616119168.htm
[6] Zie over Fedict :Het Laatste Nieuws, 3 maart 2014. Zie ook het departement LNE van de Vlaamse Overheid.
[7] http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds
[8] Gazet van Antwerpen, 11 maart 2014, "ING wil info over koopgedrag klanten doorspelen aan derden"
[9] http://webwereld.nl/big-data/82349-google-staakt-gedwongen-dataminen-studentenmail?
"Ook belooft hij deze lijn door te trekken naar de andere Apps-diensten, zoals Google Apps for Business en Google Apps for Government. Wanneer dat gebeurt wordt niet vermeldt." Het is niet zeker of dit ook garanties zal bieden voor de Europese burger.
[10] http://webwereld.nl/beveiliging/79064-microsoft-dwingt-duits-windows-backdoorartikel-offline
http://webwereld.nl/beveiliging/80709-nsa-heeft-backdoor-voor-iphones?
[11] hhttp://datanews.knack.be/ict/nieuws/topman-van-cisco-doet-zijn-beklag-bij-obama-over-nsa/article-4000628648701.htm (oa ivm Belgacom-BICS)
[12] http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

- een rechter – ook een Europese - kan gegevens opvragen aan de cloudaanbieder en u weet als eigenaar van de gegevens van niets (ongeacht de contractuele bepalingen of zelfs met een uitdrukkelijk daarin opgenomen voorbehoud)[13]

- Amerikaanse cloudproviders: grootschalige screening van clouddata met gegevens van Europese burgers bij Amerikaanse ondernemingen of ondernemingen met een link met Amerika. De opslaglocatie is niet doorslaggevend! Dit is mogelijk op basis van Amerikaanse wetgeving, namelijk de Patriot Act en FISA Amendments act, er moet zelfs geen sprake zijn van terrorisme of zware criminaliteit [14].

[13] http://www.reuters.com/article/2014/04/25/us-usa-tech-warrants-idUSBREA3O24P20140425 (data MS in Dublin)
[14] http://www.v-ict-or.be/nieuws/data-in-de-cloud-hou-rekening-met-de-amerikaanse-wetgeving